

REMARKS

The present application was filed on January 29, 2002 with claims 1 through 25. Claims 1 through 24 are presently pending in the above-identified patent application. Claims 13, 24 and 25 are proposed to be amended.

In the Office Action, the Examiner rejected claims 1, 13 and 22-25 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 and 6 of United States Patent Number 6,708,893. In addition, the Examiner rejected claims 1-3, 6, 9-15 and 19-25 under 35 U.S.C. §102(b) as being anticipated by Hadfield et al., "Windows NT Server 4 Security Handbook," (1997) (hereinafter, referred to as "h"). The Examiner indicated that claims 4, 5, 7, 8, and 16-18 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claim.

Double Patenting Rejection

The present application is owned by Avaya Technology Corp. and U.S. Patent Number 6,708,893 is believed to be owned by Lucent Technologies Inc. Thus, Applicants query whether the appropriate rejection is under Section 103. In any event, the analysis and outcome is the same. The present invention is not disclosed or suggested by, and is not obvious based on United States Patent Number 6,708,893.

Among other differences, claims 1 and 6 of United States Patent Number 6,708,893 do not require authenticating a user to one or more groups using "user information stored in a computer file *associated with said user*," as required by each independent claim of the present application, as amended.

Thus, Applicants respectfully request withdrawal of the double patenting rejection.

Independent Claims 1, 13 and 22-25

Independent claims 1, 13 and 22-25 were rejected under 35 U.S.C. §102(b) as being anticipated by Hadfield. With regard to claims 1, 13 and 22-25, the Examiner asserts that Hadfield discloses computationally verifying an identity of said user; and computationally verifying a membership of said user with said one or more groups, wherein said verifying computations are performed substantially simultaneously using user information stored in a computer file associated with said user.

With regard to this final limitation “wherein said verifying computations are performed substantially simultaneously using user information stored in a computer file associated with said user,” the Examiner merely asserts that Hadfield authenticates a user’s identity and its membership to any group with a single log-on process. The Examiner has not asserted that Hadfield uses “user information stored in a computer file associated with said user,” for these computations.

In fact, Hadfield does not use “user information stored in a computer file *associated with said user*,” as required by each independent claim, as amended. Rather, Hadfield uses centralized information stored in an “**account database**.” The Windows login is based on the security profile stored in the account database. During the log-on, the user supplies a name and password that is “validated against an account database.” See, Hadfield at page 168, lines 6-7. The database used for validation is said to depend on “several factors.” *Id.* at lines 10-11. When the user is attempting to log on to a Windows NT Server, as relevant here, “the account name and password are compared with the domain's account database. If the server is a member of a trusting domain, the user also is given the option of authenticating against the trusted domain's account database.” *Id.* at lines 12-15.

A characteristic of this Hadfield approach is that the systems that can be logged on is based on the information stored in the account database. The security is based on the “security of the system” where the account database is stored. If an attacker can get into the system, then the user profile can be compromised.

The present invention, on the other hand, uses “user information stored in a computer file *associated with said user*,” as required by each independent claim, as amended. As set forth in the original specification at page 5, lines 4-8, “the smart card 215 includes a user group membership database 300 that records information for each group to which a user is registered. In an alternate implementation, the user group membership database 300 may be stored as a computer file, for example, in the data storage device 220.” Thus, in the exemplary embodiments, the user information is stored on a smart card 215 associated with the user or in the data storage device 220 on the user’s computing device 200. (See also, claims 10 and 11).

For a Windows NT login, the authentication must be checked against the account database, so the authentication decision can only be made by entities having access to the account database. The present invention can be applied to the user information obtained from the "user information stored in a computer file *associated with said user*," as required by each independent claim, as amended.

Thus, Hadfield does not disclose or suggest authenticating a user to one or more groups using "user information stored in a computer file *associated with said user*," as required by each independent claim, as amended.

Applicants respectfully request the withdrawal of the rejection of independent claims 1, 13 and 22-25.

Dependent Claims 2-12 and 14-21

Claims 2-12 and 14-21 are dependent on independent claims 1 and 13, and are therefore patentably distinguished over Hdfield because of their dependency from independent claims 1 and 13 for the reasons set forth above, as well as other elements these claims add in combination to their base claim.

The Examiner has already indicated that claims 4, 5, 7, 8, and 16-18 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claim.


All of the pending claims following entry of the amendments, i.e., claims 1-25, are in condition for allowance and such favorable action is earnestly solicited.

If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this application, the Examiner is invited to contact the undersigned at the telephone number indicated below.

The Examiner's attention to this matter is appreciated.

Date: January 12, 2006

Respectfully submitted,



Kevin M. Mason
Attorney for Applicants
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560